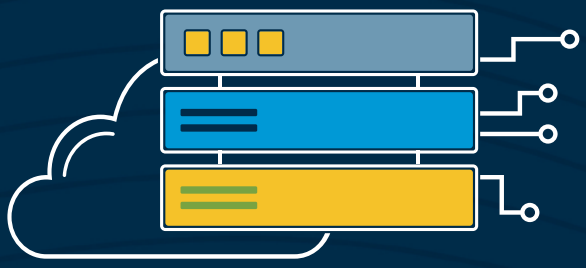
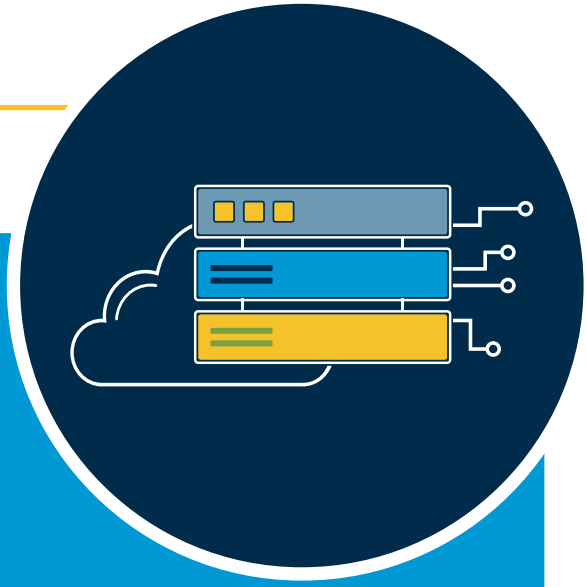


Recopilación de información y presentación de informes sobre amenazas a la seguridad de los nombres de dominio (DNSTICR)

Enero de 2022

Corporación para la Asignación de Nombres y Números en Internet

ICANN



¿Qué contiene esta guía?

¿Qué es el Sistema de Nombres de Dominio?

El **Sistema de Nombres de Dominio (DNS)** ayuda a los usuarios a ubicarse en Internet. Cada dispositivo o sitio web en Internet tiene una dirección única – como un número de teléfono. Esta dirección es una complicada serie de números, o una serie de números y letras denominada **dirección IP**. IP significa Protocolo de Internet (por sus siglas en inglés).

Las direcciones IP son difíciles de recordar. El DNS facilita la navegación por Internet.

Las direcciones IP son difíciles de recordar. El DNS facilita la navegación por Internet al permitir que los usuarios escriban letras que resultan familiares – el **nombre de dominio** – en lugar de la **dirección IP.** Por ejemplo, solo necesita escribir **https://icann.org** para acceder al sitio web de la ICANN, en lugar de su **dirección IP – 192.0.43.7**

¿Qué son las amenazas a la seguridad del DNS?

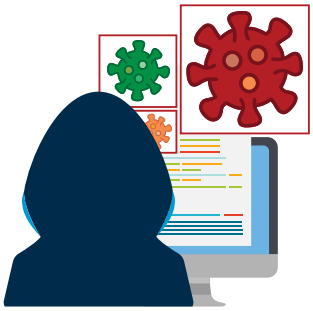
Existen varias formas de **uso indebido** relacionado con el contenido en el espacio de Internet. Algunos de estos usos indebidos incluyen sitios web que proporcionan una plataforma para actividades ilegales como la explotación infantil y el tráfico de personas. Otros promueven el ciberacoso o son un refugio digital para la venta de productos inexistentes o falsos.

Sin embargo, el ámbito de competencia de la ICANN excluye la regulación del contenido de Internet.

La organización de la ICANN centra sus esfuerzos en las **amenazas a la seguridad del DNS** específicas, que tienen un alcance más limitado que el uso indebido relacionado con el contenido. Entonces, ¿qué son las amenazas a la seguridad del DNS?

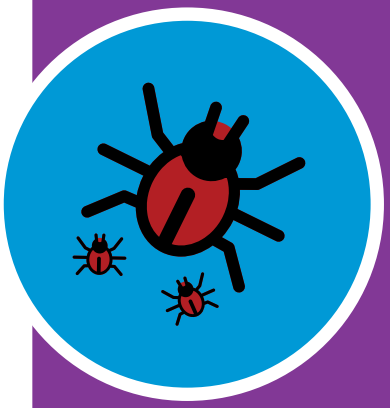
Las amenazas a la seguridad del DNS incluyen cualquier actividad maliciosa que tenga como objetivo impactar la infraestructura del DNS o hacer que el DNS funcione de manera no deseada.

Recopilación de información y presentación de informes sobre amenazas a la seguridad de los nombres de dominio (DNSTICR)



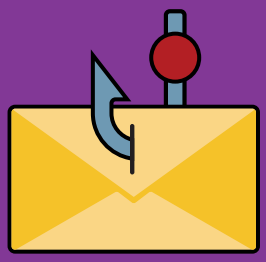
El objetivo del proyecto de **recopilación de información y presentación de informes sobre amenazas a la seguridad de los nombres de dominio (DNSTICR)** es elaborar informes sobre registraciones recientes de dominios que, según cree la organización de la ICANN, están utilizando la pandemia de COVID-19 para campañas de phishing o malware.

Estos informes contienen las pruebas que llevan a la organización de la ICANN a creer que los dominios se están utilizando de forma maliciosa. Junto con otra información de referencia, los informes ayudan a los registradores responsables a determinar el curso de acción correcto.



El proyecto DNSTICR está diseñado específicamente para buscar inyecciones de malware e intentos de phishing.

Malware
Se trata de programas informáticos instalados en un dispositivo sin el consentimiento del usuario que interrumpen el funcionamiento del dispositivo, recopilan información sensible o acceden a sistemas informáticos privados. El malware incluye virus, spyware, ransomware y otros programas informáticos no deseados.



Phishing
Ocurre cuando un atacante engaña a una víctima para que revele información personal, corporativa o financiera sensible (números de cuenta, ID de inicio de sesión, contraseñas, etc.), mediante el envío de correos electrónicos fraudulentos o similares, o bien atrayendo a los usuarios hacia copias falsas de sitios web.

El proyecto DNSTICR no está pensado para detectar las siguientes prácticas maliciosas relacionadas con Internet:

Botnets

Conjuntos de computadoras conectadas a Internet que fueron infectadas con malware y recibieron un comando para realizar actividades bajo el control de un administrador remoto.

Pharming

La redirección de usuarios a sitios o servicios fraudulentos, generalmente a través del secuestro o envenenamiento del DNS.

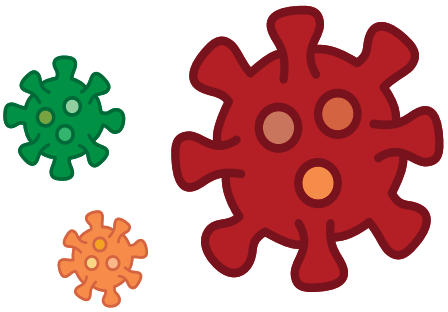
- El secuestro del DNS se produce cuando los atacantes utilizan malware para redirigir a las víctimas al sitio del atacante en lugar del sitio solicitado inicialmente.
- El envenenamiento del DNS hace que un servidor o resolutor del DNS responda con una dirección IP falsa que contiene un código malicioso. El phishing se diferencia del pharming en que este último implica la modificación de las entradas del DNS, mientras que el primero engaña a los usuarios para que introduzcan información personal.

Spam (cuando se utiliza para propagar otras amenazas a la seguridad del DNS)

Correo electrónico masivo no solicitado, enviado sin el permiso del destinatario y como parte de un conjunto de mensajes que tienen un contenido sustancialmente idéntico. Un correo electrónico genérico no solicitado por sí solo no constituye una amenaza para la seguridad del DNS, pero sí lo sería si formara parte de un esquema de phishing.

Orígenes del proyecto DNSTICR

Durante la **pandemia de COVID-19**, los delincuentes llevaron a cabo actividades de phishing contra las personas vulnerables, los desatentos, los ancianos, los niños y los más desfavorecidos. Estos delincuentes atacan a víctimas en todo el mundo y en muchos idiomas para robarles dinero e información personal.



Los delincuentes y estafadores llaman, envían correos electrónicos o envían mensajes de texto a las víctimas para engañarlas y lograr que revelen su información personal, o bien para que compren comprobantes de vacunación, pruebas o tratamientos para COVID-19 que son falsos.

Para combatir el phishing y el malware en Internet relacionado con la COVID-19, la organización de la ICANN desarrolló el proyecto **DNSTICR**. Realiza búsquedas e informa a los registradores sobre las actividades potencialmente maliciosas de los nombres de dominio y su contexto. Proporciona otra capa de defensa en la lucha de la organización de la ICANN para proteger a los usuarios de Internet de las amenazas a la seguridad del DNS.

A medida que la pandemia continúa, se actualizan los términos y temas buscados a través del proyecto DNSTICR. Esta actualización es un proceso técnico relativamente sencillo. Por ejemplo, los términos adicionales incluyen **“pasaporte”,** en relación con los **pasaportes sanitarios**utilizados en algunos países, e **“ivermectina**”, un medicamento antiparasitario que se ha asociado a la pandemia.

Otros términos podrían incluir los títulos de destacados programas relacionados con la COVID-19, patrocinados por los gobiernos y destinados a brindar ayuda a las personas necesitadas. También se incorporan términos más genéricos como “respiradores”, “máscaras N95” y “desinfectantes”.

Sin embargo, la organización de la ICANN carece de los recursos o la autoridad para verificar si todos los sitios que ofrecen estos suministros son legítimos.

Ayúdenos a proteger a la Internet de los intentos de malware y phishing relacionados con la COVID-19 en su región del mundo.

¿Es usted proveedor de servicios sanitarios, gestor financiero, regulador gubernamental, responsable del desarrollo de políticas, funcionario de la seguridad pública o profesional de la seguridad?

¡Necesitamos su ayuda!

Así es como podemos trabajar juntos para proteger a los usuarios de Internet de las amenazas a la seguridad del DNS:

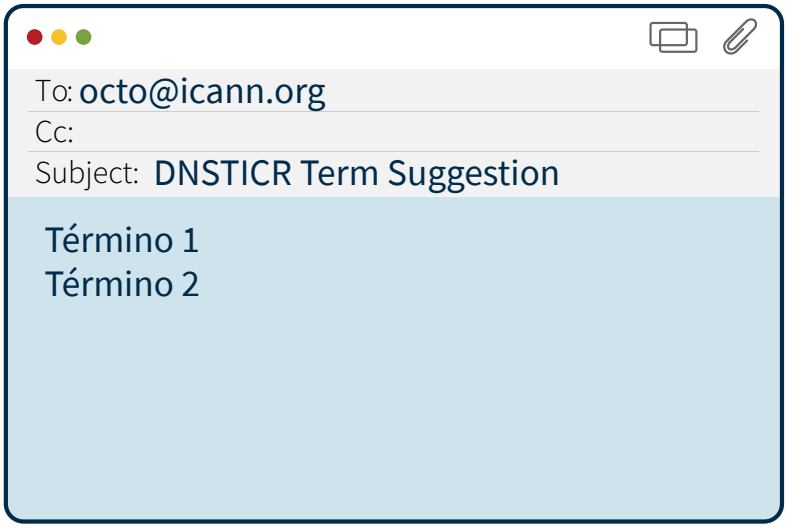
Paso 1
Arme una lista de palabras y conjuntos de caracteres en su lengua materna relacionados con la pandemia de COVID-19 que se estén utilizando o puedan utilizarse en su región para atacar a personas u organizaciones.

Paso 2
Envíe su lista por correo electrónico a **octo@icann.org** con el siguiente asunto: **Sugerencias de términos para DNSTICR**

Las nuevas sugerencias deben enviarse una por cada línea en el cuerpo del correo electrónico.

Por ejemplo:
Término 1
Término 2

Si los términos requieren una explicación, agregue la explicación después de su lista de términos.



Obtenga información sobre el proyecto de recopilación de información y presentación de informes sobre amenazas a la seguridad de los nombres de dominio (DNSTICR) y sobre cómo puede contribuir para que Internet sea un lugar más seguro.

Más información
Visite nuestra página web dedicada al proyecto DNSTICR:
https://www.icann.org/dnsticr

Explorar
Conozca las iniciativas de la organización de la ICANN para mitigar las amenazas a la seguridad del DNS:
https://www.icann.org/dnsabuse

Acrónimos y términos
Haga clic en los siguientes enlaces para obtener más información sobre los acrónimos y términos utilizados en esta guía a través de la función de acrónimos y términos de la ICANN:
https://go.icann.org/acronyms

Nombre de dominio
Etiqueta de nombre de dominio
Sistema de Nombres de Dominio (DNS)
Protocolo de Internet (IP)
Dirección de Protocolo de Internet
Protocolo de Internet versión 4 (IPv4)
Protocolo de Internet versión 6 (IPv6)

VÍAS DE CONTACTO

https://icann.org
flickr.com/icann
@icann
linkedin.com/company/icann
facebook.com/icannorg
soundcloud.com/icann
youtube.com/icannnews
instagram.com/icannorg

O visite nuestra página dedicada a las redes sociales:
https://go.icann.org/socialmedia